



DKIMセットアップガイド

(新規／既存のお客様向け)

2024/5/10

Canon

キヤノンマーケティングジャパン株式会社

目次

1. はじめに
2. 送信ドメイン認証（SPF／DKIM／DMARC）とは
3. Mailセキュリティ・クラウドによる送信ドメイン認証対応
4. 設定作業の段取りについて（概要）

Step1. SPFの登録

- SPFレコードの登録について
- SPFレコードの確認と登録
- SPFレコードの設定確認

Step2. DKIMの登録

- DKIMレコードの登録について
- DKIMレコードの確認と登録
- DKIMレコードの設定確認

Step3. WEBサイトからの登録完了申請

- WEBサイトからの登録完了申請

Step4. DKIM秘密鍵の登録（弊社作業）

- 弊社作業について

Step5. SPF／DKIMの動作確認

- SPF／DKIMの動作確認について
- SPF／DKIMの動作確認

Step6. DMARCの登録（任意）

- DMARCレコードの登録について
- DMARCレコードの確認と登録
- DMARCレコードの設定確認
- DMARCの動作確認について
- DMARCの動作確認

Appendix

- 導入後の注意事項

1. はじめに

- この度は、GUARDIANWALL Mailセキュリティ・クラウド DKIMオプション（以降、DKIMオプション）をお申込みいただきありがとうございます。
- 本資料は、GUARDIANWALL Mailセキュリティ・クラウドのご契約が新規／既存にかかわらずDKIMオプションの運用を開始いただくまでの手順をご紹介します。
- 新規のお客様は本手順実施前に、スタートアップガイドを実施ください。

2. 送信ドメイン認証 (SPF/DKIM/DMARC) とは

- 送信ドメイン認証技術とは、SPF/DKIM/DMARCがございます。期待できる効果は以下の通りです。

SPF (Sender Policy Framework)

送信元のメールサーバーの IP アドレスを検証し、正規なメールサーバーから送信されたメールか否かを判断する仕組みです。メールを受信したメールサーバーが、送信元ドメインを管理するDNSサーバーへ問い合わせを行い、実際に送信されてきたメールサーバーのIPアドレスと照合します。一致しなければ、正規メールではないと判断します。

DKIM (DomainKeys Identified Mail)

電子署名を利用してメールが改ざんされていないことを検証する仕組みです。メール送信サーバーは秘密鍵を利用して電子署名したメールを送信し、メール受信サーバーは電子署名に記載されたドメインのDNSサーバーに問い合わせを行い、公開鍵を取得し電子署名を検証しメールが改ざんされていないか検証します。改ざんされていないと判断されると電子署名（秘密鍵）を解除するための公開鍵を付与してメール受信サーバーに送られ受信者へ届きます。

DMARC (Domain-based Message Authentication, Reporting and Conformance)

SPFやDKIM署名での認証に失敗したときにそのメールをどのように処理するのかを設定をする仕組みです。「メールを隔離（迷惑メール振り分け）・受信拒否・何もしない（認証に失敗していても受信する）」といったアクションを事前に定義しておき、SPFやDKIM署名での認証に失敗したメールに対し、アクションを実行します。

3. Mailセキュリティ・クラウドによる送信ドメイン認証対応

- GUARDIANWALL Mailセキュリティ・クラウドで対応可能な送信ドメイン認証は、SPF／DKIM／DMARCとなっております。

SPF

弊社のクラウドサービスご利用時に**必須で**設定いただく項目となります。
お客様のDNSサーバーの設定を変更いただき、ご利用いただきます。

DKIM

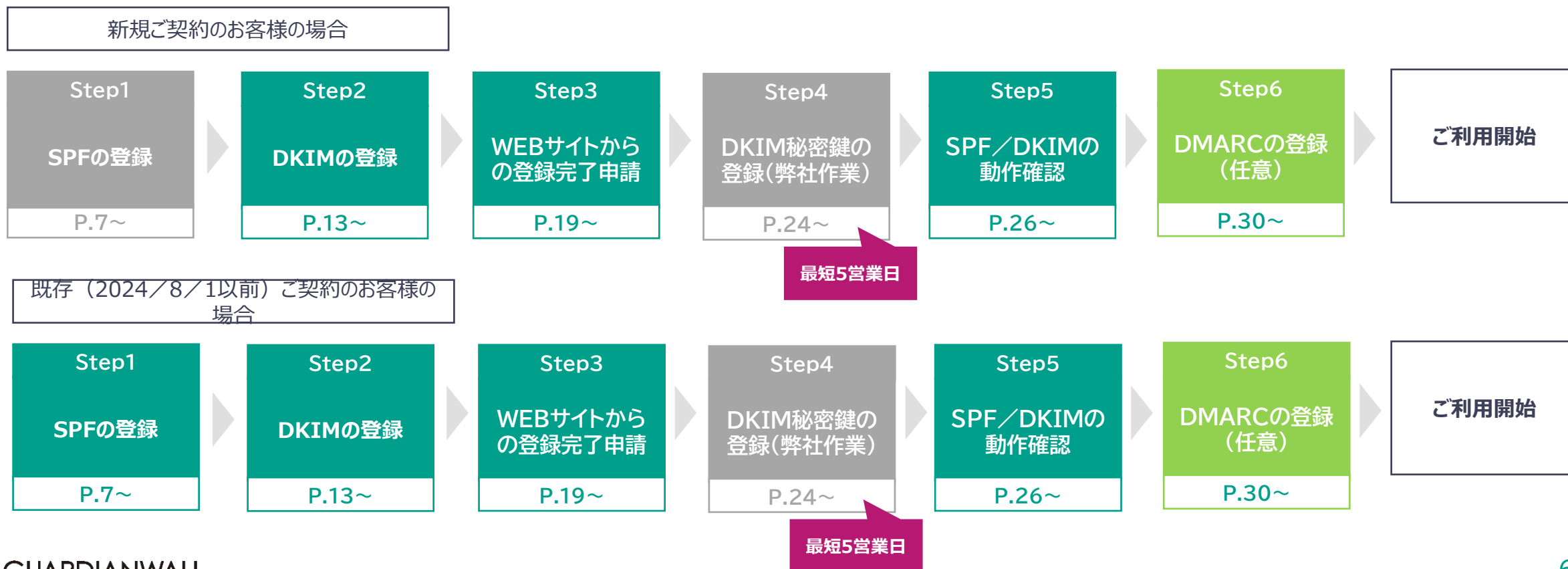
オプション製品となっております。ご利用いただくには、**別途お申し込みが必要となります。**
お客様のDNSサーバーの設定を変更いただき、ご利用いただきます。

DMARC

SPFとDKIMを連動させてご利用いただきます。**実施されたいお客様のみ任意で実施いただけます。**
実施の際にお申し込みや弊社への連絡は必要ありません。
お客様のDNSサーバーの設定を変更いただき、ご利用いただきます。
※GoogleのGmailアカウントに送信する場合は、Googleのメール送信ガイドラインに沿って対応いただく必要があります。

4. 設定作業の段取りについて（概要）

- 本資料は、SPF／DKIM／DMARCの設定手順をご紹介します。設定の流れは以下の通りです。
- の色の箇所がお客様にて実施いただく作業となります。
- 新規ご契約のお客様の場合、DKIM対応用SPFレコードは登録済みのため「Step1 SPFの登録」作業は不要です。
- 「Step4 DKIM秘密鍵の登録（弊社作業）」は、**最短で5営業日**いただいております。



Step1. SPFの登録

SPFレコードの登録について

- DKIMオプションをご利用いただくには、DNSサーバーに登録されているSPFレコードをDKIM対応用のSPFレコードへ変更いただく必要があります。

※ SPFレコード登録について

- DKIMをご利用の場合と、ご利用いただかない場合で設定の内容が異なります。
- 新規のお客様については、GUARDIANWALL Mailセキュリティ・クラウドのスタートアップガイドを実施していただいた際に、DKIM対応用のSPFレコードを登録いただいておりますので本手順の実施は必要ありません。
- すでにGUARDIANWALL Mailセキュリティ・クラウドの各種サービスをご利用中の場合、DKIM未対応のSPFレコードを登録されていますので、DKIMオプションお申込み時にサポート窓口よりご案内しているDKIM対応用のSPFレコードへ修正する必要があります。本手順に沿って登録してください。

SPFレコードの確認と登録

手順1. お手元に**SPFレコード情報**をご用意ください。

※ DKIMオプションお申込み時にサポート窓口よりご案内しているメールに記載されています。

SPFレコード情報 (例)

```
include:_prspfXX.guardianwall.jp
```

SPFレコードの確認と登録

手順2. SPFレコードを登録します。

自社にてDNSサーバーを運用されている場合は、運用に沿って変更してください。

DNSプロバイダーをご利用の場合は、変更依頼を実施してください。

※ SPFで利用できるパラメータ・タグについては、「SPFレコードの設定に利用できる一部のタグについてご紹介」(P.12) を参照ください。

※ 複数ドメインでGUARDIANWALL Mailセキュリティ・クラウドを実施する場合は、すべてのドメインへSPFレコードを追加する必要があります。

依頼文 (例)

導入を検討しているメールセキュリティサービスを利用するためにSPFレコードの追加が必要です。
以下を追加いただけますでしょうか。

■ SPFレコード

Type : TXT
Name : <ドメイン情報>
Value : v=spf1 <SPFレコード情報> ~all
TTL : 1800



SPF、DKIM、DMARCの登録をプロバイダーへ依頼する場合は、まとめて依頼しても問題ありません。

DKIMは、P.16から依頼文 (例) を確認してください。

DMARCは、P.33から依頼文 (例) を確認してください。

手順3. 以上でSPFの登録は完了です。

続けて「SPFレコードの設定確認」(P.11) に進んでください。

SPFレコードの設定確認

手順1. 設定内容を確認をします。

コマンドプロンプトまたはターミナルより以下のコマンドを実行します。

※ <ドメイン情報>はSPFレコードを設定したドメインに書き換えてください。

```
nslookup -type=TXT <ドメイン情報>
```

手順2. 以下は表示の一例です。設定したSPFレコードが表示されれば設定完了です。

```
<ドメイン情報>.          1800  IN      TXT     "v=spf1 <SPFレコード情報> ~all"
```

手順3. 以上でSPFの設定確認は完了です。

続けて「Step2. DKIMの登録」(P.13)に進んでください。



SPFレコードの設定に利用できる一部のタグについてご紹介

SPFで利用できるタグ

タグ	指定する値	内容
v	SPF1	<ul style="list-style-type: none">SPFのバージョンを記載する
all	+ / - / ~ / ?	<ul style="list-style-type: none">すべての送信元ホストにマッチするSPFレコードの末尾に置かれ、デフォルトの動作を定義するために利用される値を指定する<ul style="list-style-type: none">+ : 当該ドメインの送信メールサーバとして認証する (Pass)- : 当該ドメインの送信メールサーバとして認証しない (Fail)~ : 認証情報を公開しているが、正当なメールであっても認証失敗する可能性もある (SoftFail)? : 認証情報を公開しない (Neutral)
include	ドメイン名	<ul style="list-style-type: none">引数に与えられたドメインのSPFレコードを使って認証処理を行う
ip4	IPv4ネットワークアドレス	<ul style="list-style-type: none">送信元ホストのIPアドレスが、引数に指定されるIPv4のネットワークに含まれているか認証を行うIPアドレスにマッチする場合、認証成功となる
ip6	IPv6ネットワークアドレス	<ul style="list-style-type: none">送信元ホストのIPアドレスが、引数に指定されるIPv6のネットワークに含まれているか認証を行うIPアドレスにマッチする場合、認証成功となる
redirect	ドメイン名	<ul style="list-style-type: none">リダイレクト先のドメインのSPFレコードを用いて認証させる場合に設定する

Step2. DKIMの登録

DKIMレコードの登録について

- DKIMオプションをご利用いただくには、DNSサーバーにDKIMレコードを設定いただく必要があります。
- DKIMオプションお申込み時にサポート窓口よりご案内しているDKIM設定値をDNSサーバーへ本手順に沿って登録してください。

DKIMレコードの確認と登録

手順1. お手元に**DKIMレコード情報**をご用意ください。

※ DKIMオプションお申込み時にサポート窓口よりご案内しているメールに添付されている「XX_XXXX_<お客様メインドメイン名>_dkim_settings.csv」ファイルです。

DKIMレコード情報 (例)				
A列	B列	C列	D列	E列
Domain	Selector	FQDN	Record	Public_key
example.co.jp	pr1-example-exjhh8nkw3	pr1-example-exjhh8nkw3_domainkey.example.co.jp	v=DKIM1; k=rsa; p=XXXXXXXXXXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXX

DKIMレコードの確認と登録

手順2. DKIMレコードを登録します。

自社にてDNSサーバーを運用されている場合は、運用に沿って変更してください。

DNSプロバイダーをご利用の場合は、変更依頼を実施してください。

※ DKIMで利用できるパラメータ・タグについては、「DKIMレコードの設定に利用できる一部のタグについてご紹介」(P.18) を参照ください。

※ 複数ドメインでDKIMオプションを実施する場合は、すべてのドメインへDKIMレコードを追加する必要があります。

依頼文 (例)

導入を検討しているメールセキュリティサービスを利用するためにDKIMレコードの追加が必要です。
以下を追加いただけますでしょうか。

■ DKIMレコード

Type	: TXT
Name	: <B列のSelector情報>._domainkey.<A列のDomain情報>
Value	: <D列のRecord情報>
TTL	: 1800



SPF、DKIM、DMARCの登録をプロバイダーへ依頼する場合は、まとめて依頼しても問題ありません。

SPFは、P.10から依頼文 (例) を確認してください。

DMARCは、P.33から依頼文 (例) を確認してください。

手順3. 以上でDKIMの登録は完了です。

続けて「DKIMレコードの設定確認」(P.17) に進んでください。

DKIMレコードの設定確認

手順1. 設定内容を確認をします。

コマンドプロンプトまたはターミナルより以下のコマンドを実行します。

※ <A列のDomain情報>、<B列のSelector情報>、<D列のRecord情報>は、「XX_XXXX_<お客様メインドメイン名>_dkim_settings.csv」ファイルを参照し、書き換えてください。

```
nslookup -type=TXT <B列のSelector情報>._domainkey.<A列のDomain情報>
```

手順2. 以下は表示の一例です。設定したDKIMレコードが表示されれば設定完了です。

```
<B列のSelector情報>._domainkey.<A列のDomain情報>. 1800 IN TXT " v=DKIM1; k=rsa;  
p=XXXXXXXXXXXXXXXXXXXXXXXXX"
```

手順3. 以上でDKIMの設定確認は完了です。

続けて「Step3. WEBサイトからの登録完了申請」(P.19)に進んでください。



DKIMレコードの設定に利用できるパラメータと一部のタグについてご紹介

DKIMの設定パラメータ

パラメータ	指定する値	内容
Selector	pr-xxxxxxx	<ul style="list-style-type: none">• 弊社が発行する値• テナント毎にランダムでユニークな値を発行する
_domainkey	_domainkey	<ul style="list-style-type: none">• 全てのDKIMレコードに必須で設定する
Domain	例) example.co.jp	<ul style="list-style-type: none">• ドメイン名は送信元になるドメインを指定する
TTL	例) 600	<ul style="list-style-type: none">• TTLはレコードがリフレッシュされるまでの有効時間を示す• DKIMレコードのTTLは通常数分• 秒単位で指定する

DKIMで利用できるタグ

タグ	指定する値	内容
v	DKIM1	<ul style="list-style-type: none">• DKIMのバージョンを記載する• 設定することが推奨されるが、省略可能
k	rsa	<ul style="list-style-type: none">• 電子署名の作成の際に利用できる鍵の形式を指定する• 現在はRSAのみサポートしており、省略可能
t	y / s	<ul style="list-style-type: none">• フラグを指定するy : 試験モードであることを示すs : ドメイン名は一致する必要がある
p	公開鍵のデータ	<ul style="list-style-type: none">• 鍵データを指定する• 弊社にてご案内する公開鍵の情報を指定する

Step3. WEBサイトからの登録完了申請

WEBサイトからの登録完了申請

手順1. SPF/DKIMの完了申請を実施します。

以下のURLへアクセスします。

- ※ 申請を受け付け次第、弊社にてDKIMの秘密鍵登録を行います。
- ※ 弊社作業には**最短5営業日**いただきます。

https://security-support.canon-its.jp/helpdesk?category_id=299&site_domain=gwc

The screenshot shows the Canon IT Solutions website's support portal for GuardianWall Mail Security Cloud. The page is in Japanese and displays a form for a DKIM registration application. The form includes fields for company name, contact number, email, and a confirmation checkbox. A detailed notice explains the process and the 5-business-day timeline.

Canon キヤノン ITソリューションズ株式会社

GUARDIANWALL

サポート情報 (GUARDIANWALL Mailセキュリティ・クラウド)

GUARDIANWALL Mail セキュリティ・クラウド カテゴリ一覧 > お問い合わせ(DKIM利用開始申請) > お問い合わせ内容入力

個人情報の取り扱いについて

キヤノンITソリューションズ株式会社(以下「当社」といいます。)では、お客さまからご提供いただくお客さまの個人情報(住所、氏名等のお客さまの個人的な情報)を、下記の通り取り扱いいたします。

【利用目的に関して】
当社は、ご提供いただきました個人情報を今回のお問い合わせに関する回答処理のために利用いたします。また、当社のイベント/製品/サービス/サポート情報の送付など、営業活動に必要な範囲内で利用し、ご本人の同意なく利用目的以外に利用いたしません。

お問い合わせ内容入力

カテゴリ	お問い合わせ(DKIM利用開始申請)
会社名 [必須]	弊社に届け出たい会社名をご入力ください。 例) キヤノン ITソリューションズ株式会社
受付番号 [必須]	申込書受付時に弊社よりお伝えしている「受付番号」を入力してください。 例) AA0000-0
E-mail [必須]	例) canon.taro@canon-its.co.jp
E-mail (確認) [必須]	例) canon.taro@canon-its.co.jp 確認のため、もう一度メールアドレスを入力してください
DKIMレコード登録確認 [必須]	<input type="checkbox"/> ドメインを管理する DNS に DKIM レコードを登録しました
問い合わせ内容 [必須]	本 DKIM 利用開始申請により弊社側設定作業を実施いたします。 以下の注意事項をご確認の上、お申込ください。 ・ DNS に DKIM レコードを設定していることをご確認ください。 正しく設定されていない場合、正しく認証されず不審メールとして扱われる場合があります。 ・ 設定作業には 最短 5 営業日 をいただいております。 (作業日の指定は出来かねます。) 設定作業完了後は本フォームに入力されたメールアドレス宛にご連絡いたします。 上記ご了承の上、本「問い合わせ内容」に「 注意事項を確認した 」旨をご記入ください。 <input type="text"/> <small>質問内容をなるべく詳細にご入力ください。</small>

内容をご確認のうえ「入力内容を確認」ボタンをクリックしてください。
ついでに、内容確認画面が表示されます。

TOPへ

サイトのご利用について 個人情報の取り扱いについて

© Canon IT Solutions Inc.

PKSH

WEBサイトからの登録完了申請

手順2. 会社名、受付番号、E-mail、E-mail（確認）を記入します。

- ※ 受付番号は、DKIMオプションお申込み時にサポート窓口よりご案内しているメールに記載されています。
ご契約がプレミアムの場合は「PR0000-0」、ご契約がベーシックの場合は「BC0000-0」の形式となっております。
- ※ E-mail（確認）には、E-mail に記載した内容と同様のアドレスを記入してください。

会社名 [必須]	弊社に届け出いただいている会社名をご入力ください。 <input type="text" value="例) キヤノン ITソリューションズ株式会社"/>
受付番号 [必須]	申込書受付時に弊社よりお伝えしている「受付番号」を入力してください。 <input type="text" value="例) AA0000-0"/>
E-mail [必須]	<input type="text" value="例) canon.taro@canon-its.co.jp"/>
E-mail（確認） [必須]	<input type="text" value="例) canon.taro@canon-its.co.jp"/> 確認のため、もう一度メールアドレスを入力してください

手順3. DKIMレコード登録確認にチェックを入れます。

DKIMレコード登録確認 [必須]	<input type="checkbox"/> ドメインを管理する DNS に DKIM レコードを登録しました
-------------------	---

WEBサイトからの登録完了申請

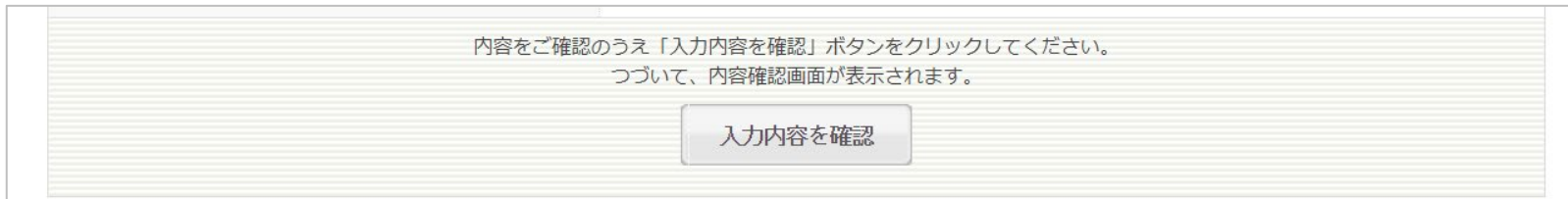
手順4. 注意事項をご確認いただき、お問合せ内容に「注意事項を確認しました」と記入します。

問い合わせ内容 [必須]	<p>本 DKIM 利用開始申請により弊社側設定作業を実施いたします。 以下の注意事項をご確認の上、お申込ください。</p> <ul style="list-style-type: none">・ DNS に DKIM レコードを設定していることをご確認ください。 正しく設定されていない場合、正しく認証されず不審メールとして扱われる場合があります。・ 設定作業には最短 5 営業日をいただいております。<u>(作業日の指定は出来かねます。)</u> 設定作業完了後は本フォームに入力されたメールアドレス宛にご連絡いたします。 <p>上記ご了承の上、本「問い合わせ内容」に「<u>注意事項を確認した</u>」旨ご記入ください。</p> <div data-bbox="912 886 1793 1086" style="border: 1px solid #ccc; height: 140px; width: 100%;"></div> <p>質問内容をなるべく詳細にご入力ください。</p>
--------------	--

注意事項

WEBサイトからの登録完了申請

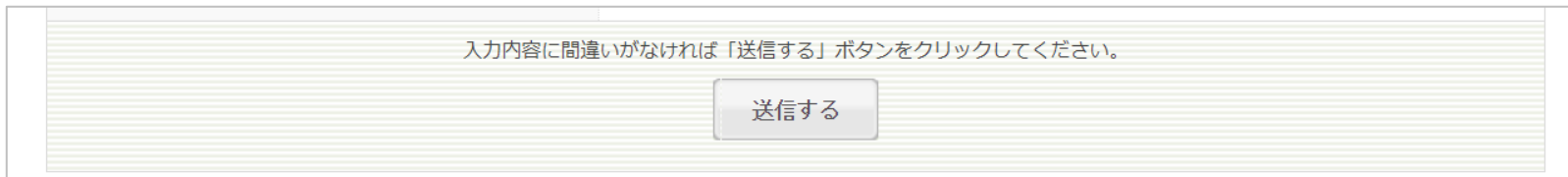
手順5. すべての項目が記載できたら、「入力内容を確認」をクリックします。



内容をご確認のうえ「入力内容を確認」ボタンをクリックしてください。
つづいて、内容確認画面が表示されます。

入力内容を確認

手順6. 表示された記載内容をご確認いただき、「送信する」をクリックします。



入力内容に間違いがなければ「送信する」ボタンをクリックしてください。

送信する

手順7. 以上でWEBサイトからの登録完了申請は完了です。

続けて、「Step4. DKIM秘密鍵の登録（弊社作業）」（P.24）へ進んでください。

Step4. DKIM秘密鍵の登録（弊社作業）

弊社作業について

お客様にてWEBサイトからの登録完了申請が完了したら、

ご連絡受領後、弊社にて作業を実施いたします。

最短5営業日かかりますので、作業が終わるまでお待ちください。

※ DKIMオプションをお申込みいただいたドメインに対してのみ、作業を実施いたします。

弊社での作業完了後、サポート窓口より設定完了の通知メールを送付いたします。

メールを受領したら、「Step5. SPF／DKIMの動作確認」(P.26)へ進んでください。

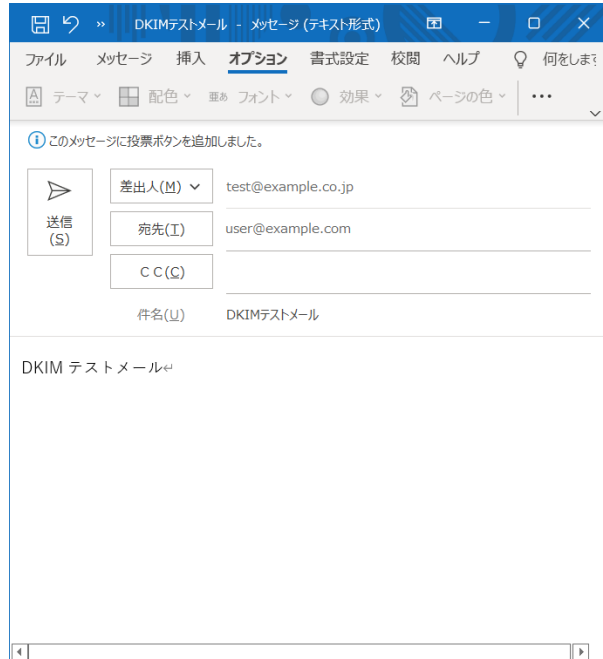
Step5. SPF/DKIMの動作確認

SPF／DKIMの動作確認について

- メールのヘッダー情報からSPF／DKIMの登録を確認する方法をご紹介します。
- 外部のオンラインチェックツールを使用して確認することも可能です。オンラインチェックツールをご利用の場合は、各サイトでのご利用方法に則って実施ください。

SPF／DKIMの動作確認

手順1. DKIMを設定したドメインから、外部ドメイン宛てにメールを送信します。



手順2. メールを受信します。

SPF／DKIMの動作確認

手順3. 受信したメールのヘッダー情報を確認します。

「Authentication-Results」ヘッダーの値に「spf=pass」「dkim=pass」の記載があるか確認してください。

※ 「spf=pass」または「dkim=pass」となっていない場合、DNSサーバー上のいずれかの設定が間違っている可能性がありますので、DNSサーバーの設定値をご確認ください。

(前略)

```
Authentication-Results: spf=pass (sender IP is 192.168.1.1)
smtp.mailfrom=example.co.jp; dkim=pass (signature was verified)
header.d= example.co.jp;dmarc=pass action=none
header.from= example.co.jp;compauth=pass reason=100
```

(後略)

手順4. 以上でSPF／DKIMの動作確認は完了です。

SPF／DKIMをご利用の場合、すべての設定は完了です。ご利用を開始してください。

DMARCを設定するお客様は、続けて「Step6. DMARCの登録（任意）」(P.30)に進んでください。

Step6. DMARCの登録（任意）

DMARCレコードの登録について

- GUARDIANWALL Mailセキュリティ・クラウドでDMARCをご利用いただくには、DNSサーバーにDMARCレコードを設定する必要があります。本手順に沿って登録してください。

DMARCレコードの確認と登録

- 手順1. DMARCご利用の場合、レポートが送信されます。
送信先のアドレスである「レポート用メールアドレス」と「NGレポート用メールアドレス」を決めてください。

タグ	説明	設定値
レポート用メールアドレス	DMARCの集計レポートの送信先アドレスを設定します（複数指定可能）	
NGレポート用メールアドレス	DMARCの失敗レポートの送信先アドレスを設定します（複数指定可能）	

DMARCLレコードの確認と登録

手順2. DMARCLレコードを登録します。

自社にてDNSサーバーを運用されている場合は、運用に沿って変更してください。

DNSプロバイダーをご利用の場合は、変更依頼を実施してください。

※ DMARCで利用できるパラメータ・タグについては、「DMARCLレコードの設定に利用できる一部のタグについてご紹介」(P.38) を参照ください。

※ 複数ドメインでDMARCを実施する場合は、すべてのドメインへDMARCLレコードを追加する必要があります。

依頼文 (例)

メールセキュリティ向上のためにDMARCLレコードの追加が必要です。
以下を追加いただけますでしょうか。

■ DMARCLレコード

Type : TXT

Name : _dmarc.<ドメイン情報>

Value : v=DMARC1; p=none; rua=mailto:<レポート用メールアドレス>; ruf=mailto:<NGLレポート用メールアドレス>

TTL : 1800



SPF、DKIM、DMARCの登録をプロバイダーへ依頼する場合は、まとめて依頼しても問題ありません。

SPFは、P.10から依頼文 (例) を確認してください。

DKIMは、P.16から依頼文 (例) を確認してください。

手順3. 以上でDMARCの登録は完了です。

続けて「DMARCLレコードの設定確認」(P.34) に進んでください。

DMARCレコードの設定確認

手順1. 設定内容を確認をします。

コマンドプロンプトまたはターミナルより以下のコマンドを実行します。

※ <ドメイン情報>はDMARCレコードを設定したドメインに書き換えてください。

```
nslookup -type=TXT _dmarc.<ドメイン情報>
```

手順2. 以下は表示の一例です。設定したDMARCレコードが表示されれば設定完了です。

```
_dmarc.<ドメイン情報>      "v=DMARC1; p=none; rua=mailto:<レポート用メールアドレス>; ruf=mailto:<NGLレ  
ポート用メールアドレス>"
```

手順3. 以上でDMARCの設定確認は完了です。

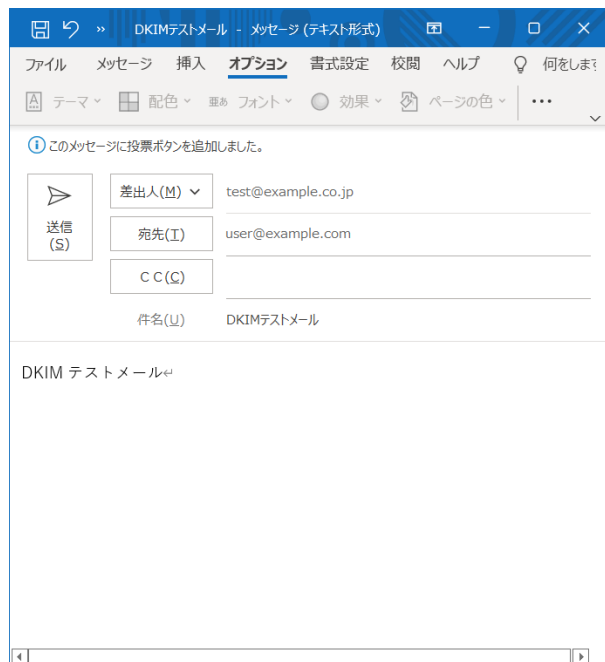
続けて、「DMARCの動作確認について」(P.35)に進んでください。

DMARCの動作確認について

- メールのヘッダー情報からDMARCの登録を確認する方法をご紹介します。
- 外部のオンラインチェックツールを使用して確認することも可能です。オンラインチェックツールをご利用の場合は、各サイトでのご利用方法に則って実施ください。

DMARCの動作確認

手順1. DMARCを設定したドメインから、外部ドメイン宛てにメールを送信します。



手順2. メールを受信します。

DMARCの動作確認

手順3. 受信したメールのヘッダー情報を確認します。

「Authentication-Results」ヘッダーの値に「dmarc=pass」の記載があるか確認してください。

※ 「dmarc=pass」となっていない場合、DNSサーバー上のSPFまたはDKIMの設定が間違っている可能性がありますので、DNSサーバーの設定値をご確認ください。

(前略)

```
Authentication-Results: spf=pass (sender IP is 192.168.1.1)
smtp.mailfrom=example.co.jp; dkim=pass (signature was verified)
header.d= example.co.jp; dmarc=pass action=none
header.from= example.co.jp; compauth=pass reason=100
```

(後略)

手順4. 以上でDMARCの動作確認は完了です。

SPF／DKIM／DMARCをご利用の場合のすべての設定は完了です。ご利用を開始してください。



DMARCレコードの設定に利用できるパラメータと一部のタグについてご紹介

DMARCの設定パラメータ

パラメータ	指定する値	内容
_dmarc	_dmarc	<ul style="list-style-type: none">全てのDMARCレコードに必須で設定する
Domain	例) example.co.jp	<ul style="list-style-type: none">送信元になるドメインを指定する
TTL	例) 600	<ul style="list-style-type: none">レコードがリフレッシュされるまでの有効時間を示すDMARCレコードのTTLは通常数分秒単位で指定する

DMARCの設定タグ

タグ	指定する値	内容
v	DMARC1	<ul style="list-style-type: none">DMARCのバージョン（現在はDMARC1）※必須
p	none / quarantine / reject	<ul style="list-style-type: none">認証に失敗した場合に受信側で実行してほしいアクション ※必須
rua	mailto:xxxxx@example.co.jp	<ul style="list-style-type: none">集計レポートの送信先アドレス（複数指定可能）
ruf	mailto:xxxxx@example.co.jp	<ul style="list-style-type: none">失敗レポートの送信先アドレス（複数指定可能）
adkim	r / s	<ul style="list-style-type: none">DKIMのアライメントモード<ul style="list-style-type: none">r : サブドメインでの一致でも可s : ドメインが完全に一致する必要がある
aspf	r / s	<ul style="list-style-type: none">SPFのアライメントモード<ul style="list-style-type: none">r : サブドメインでの一致でも可s : ドメインが完全に一致する必要がある

Appendix

導入後の注意事項

導入後の注意点は以下のとおりです。

- ① SPFレコードのDNSルックアップ回数について
- ② DKIM公開鍵のビット数について
- ③ DKIM公開鍵の変更について
- ④ 複数ドメインをご利用の場合
- ⑤ DNSサーバー負荷について
- ⑥ DKIM認証が失敗するケースについて
- ⑦ DKIM認証に失敗した場合
- ⑧ DKIM認証失敗時の調査
- ⑨ 通知メールの差出人設定について

① SPFレコードのDNSルックアップ回数について

- 弊社からご案内するSPFレコードは、DNSへの「include」のルックアップ回数が**2~3回**あります。
- ルックアップ回数をご提供するSPFレコードの内容によって変動します。
- SPFのDNSルックアップ回数制限（10回まで）に達してしまう場合、エラーとなり迷惑メールとして判定される場合やメールそのものを受付できない可能性があります。
正しくSPFレコードが登録されているにもかかわらず迷惑メールと判定されてしまう、もしくはメールが受信できない場合は、**不要なincludeが登録されていないか、DNSサーバーの設定を見直してください。**

例えば、includeの先でさらにincludeしている場合

include:spf.example.co.jp

└ include:spf.AAAA.co.jp

└ include:spf.BBBB.com include:spf.CCCC.jp

└ +ip4:192.168.1.1 └ +ip4:192.168.1.2

合計で4回のルックアップ
が発生

※ 「a」「mx」「include」「redirect」はこの制限の対象になります

② DKIM公開鍵のビット数について

- DKIM公開鍵のビット数は**2048ビット**でのご提供となります。お客様ドメインを公開しているDNSサーバーで取り扱えるTXTレコードの文字数を事業者へご確認ください。
- 弊社からご提供する2048ビット公開鍵が登録できない場合があります。

例)

- ご利用のDNSプロバイダーが、1024ビットのみしか対応していない
- DNSへ登録するDKIMレコードが256文字を超えている



1024ビットの公開鍵のご提供を実施します。弊社サポート窓口までご連絡ください。

※ 1024ビット公開鍵では2048ビット公開鍵と比べ強度が弱くなります。

※ 可能であれば、2048ビット公開鍵がご利用いただけるよう、DNSプロバイダー様とご調整をお願いします。

※ 安全性の観点から、一定期間での入替が推奨されます。弊社からは能動的にその旨ご連絡いたしませんので、お客様での管理をお願いします。

③ DKIM公開鍵の変更について

- 安全性の観点から、DKIM公開鍵を一定期間で入替することが推奨されています。弊社からは能動的にその旨ご連絡いたしませんので、お客様での管理をお願いします。
- 新しいDKIM公開鍵をご希望の場合は、弊社サポート窓口までご連絡ください。

④ 複数ドメインをご利用の場合

- DKIMのご利用は、申請書にDKIMを実施されたいドメイン情報を記載いただいておりますが、サービスでご利用いただいているすべてのドメインのDKIMレコード情報をご提供しております。
お手数ですが、ご提供したDKIMレコード情報の中から、DKIMをご利用になりたいドメインの情報を抜き出して設定してください。
- 申込書に記載いただいたドメインについてのみDKIMレコードの設定を実施いただく必要がございます。
- また、DKIMをご利用になるドメインについては、あわせてSPFレコードの変更が必要となります。
- 弊社による DKIM 適用作業は、申込書に記載いただいたドメインについてのみ実施します。

⑤ DNSサーバー負荷について

- DKIMを導入すると、以前に比べDNSサーバーへの通信負荷が高まります。
DNSクエリ（DNSサーバーへのリクエスト／問い合わせ）が失敗した場合、DKIM認証も失敗する原因になります。自社でDNSサーバーを運用している場合は、サーバースペックの見直しが必要になる場合があります。

⑥ DKIM認証が失敗するケースについて

- DKIM機能についての制限・制約として送信先メールサーバーの環境や経路によっては、DKIM認証が失敗する場合がございます。
（例：DNSがUDPモードに限定されているなど）
- 本サービスでは、IPAが定める基準に準じてセキュリティリスクの判断をしています。

⑦ DKIM認証に失敗した場合

- 受信者側の運用によっては、迷惑メールと判断され迷惑メールフォルダに振り分けられる、メール自体を受信できない、などの事象が発生することがあります。

⑧ DKIM認証失敗時の調査

- 弊社にて認証失敗した原因を調査する場合、メール検体の提供やDNSサーバーの登録情報の提供など、調査のご協力をお願いする場合があります。

⑨ 通知メールの差出人設定について

- GUARDIANWALL Mailセキュリティ・クラウドでは、運用により、送信者および管理者へ通知メールを発行します。送信元アドレスの設定が可能です。設定しない場合、エンベロープFromアドレスに何も指定がない<null>の状態となります。エンベロープFromアドレスが<null>の場合、配送出来ない可能性があります。
- DKIMオプションをご利用の場合において、エンベロープFromアドレスを元にDKIM検証を行う仕組み上、必ず設定が必要になりますので、設定を実施してください。

通知メールの差出人アドレス設定方法

プレミアムご契約の場合

- ① 管理者アカウントにて管理画面にログインします。
- ② 画面右上の「設定」をクリックします。
- ③ メニューから「システム設定」-「基本設定」をクリックします。
- ④ 管理者メール通知にある「差出人メールアドレス」にアドレスを入力し、「エンベロープFromアドレスにも使用する」にチェックを入れます。
- ⑤ 画面下部にある「更新」をクリックします。
- ⑥ ポップアップが表示されるので「OK」をクリックします。

※ ベーシックご契約の場合は、弊社から環境ご提供時に実施しておりますため不要です。

管理者メール通知	
宛先メールアドレス * ※	<input type="text" value="admin@example.co.jp"/> <input type="checkbox"/> [更新] ボタンクリック時にテストメールを送信する
差出人メールアドレス *	<input type="text" value="admin@example.co.jp"/> <input checked="" type="checkbox"/> エンベロープFromアドレスにも使用する
差出人コメント	<input type="text" value="GUARDIANWALL MailSuite"/>

ここにチェックを入れること！